

provides that carriers shall deliver post-cut-through dialed digits and notification messages for in-band and-out-band signaling over the call data channel. Appendix 1 (§ 64.1708(d), (i)(1)).

86. (c) Timely delivery of call-identifying information. Section 103(a)(2)(A) of CALEA (47 U.S.C. § 1002(a)(2)(A)) obligates carriers to provide law enforcement with access to call-identifying information "before, during, or immediately after the transmission" of the communication to which it pertains, or "at such later time as may be acceptable to the government." In addition, Section 103(a)(2)(B) requires that call identifying information be made available "in a manner that allows it to be associated with the communication to which it pertains." A carrier relies on dialing and signaling information associated with a particular call in order to process and control that call from origin to destination and termination, including any redirection signaled during the call.

87. Law enforcement currently acquires contemporaneous information regarding the processing and content of a call through its monitoring of the local loop. It is imperative for law enforcement to be able to associate the call-identifying information to the call to which it pertains in an expeditious manner so that law enforcement can promptly and accurately correlate relevant evidence, and respond in emergency and life-threatening cases. Assume, for example, that the subject places a call to a "contract killer," and that the call involves a murder that is to take place immediately. If, while intercepting the "contract murder" communication, law enforcement cannot immediately associate the call-identifying information with the communication, law enforcement officers may be unable to save a life because they are not able to identify promptly, through the acquisition of the

telephone dialing information, whom the subject had called and where that party's telephone was located.

88. The prompt receipt of call-identifying information is also critical, for example, in illegal gambling cases, where the subject typically uses a "flash hook" feature to continuously accept incoming calls being held on "call-waiting." Without expeditiously receiving the call-identifying information, law enforcement would be unable to identify the separate calls.

89. The prompt receipt of call-identifying information that is clearly associated with a particular communication is also critical for law enforcement to carry out its statutory obligation of "minimizing" the interception of non-criminal communications to promote privacy. See generally 18 U.S.C. § 2518(5). To carry out its minimization obligations, law enforcement must quickly identify all parties to a conversation, even in multi-party calls, to determine the criminal culpability of the parties to the call. If a subject makes a call to a known non-culpable person or entity, such as a relative or business that is known not to be involved in criminal activity, law enforcement should immediately minimize the interception. In a multi-party call, if a subject drops off the call or an additional subject joins the call, law enforcement must promptly recognize that these events have occurred, ascertain which subjects are party to the call, and determine what, if any, minimization procedures should be employed. Without the prompt receipt of call-identifying information these requirements cannot be met.

90. Despite the importance of prompt delivery of call-identifying information, the interim standard places no requirements on when call data is to be delivered to law enforcement. The interim standard therefore would permit carriers to deliver call-identifying information at a time other than "before, during, or immediately after" the communication -- and consequently would threaten law enforcement's traditional ability to associate call-identifying information with the communication to which it pertains. The failure of the interim standard to impose a specific delivery time requirement renders it manifestly deficient under Section 103(a)(2) of CALEA.

91. CALEA does not specify a particular time frame that would satisfy the "association" requirement of Section 103(a)(2)(B). However, the establishment of a reasonably short and objective timing requirement is essential to effectively implement that requirement and to ensure that call-identifying information is, in fact, delivered "before, during, or immediately after" a communication.

92. The proposed rule provides that carriers shall access and deliver call-identifying information to law enforcement "contemporaneously with the communications to which it pertains, or in a manner comparable to the speed with which other signaling messages are sent in the public network so that call-identifying information may be associated with the related communications." Appendix 1 (§ 64.1708(e)). Consistent with carrier network processing of call-identifying information, the proposed rule specifies an accuracy rate of 100 milliseconds (ms) for time stamps (i.e., no more than 100 ms difference between the time of the event and the time recorded in the time stamp) and

delivery "in as near real time as possible, but no later than three seconds after the occurrence of the associated call event * * * ." Id. § 64.1708(e)(1)-(3).

93. The particular timing requirements in the proposed rule are not the only ones that would satisfy Section 103(a)(2). Nevertheless, either these requirements or other reasonable and comparably effective ones are necessary. Adoption of such requirements will enable call data to be associated with the correct call and will permit law enforcement to react quickly in situations where innocent lives are threatened. For example, when a ransom call or a bomb threat call is made, the calling number will be provided quickly and will give law enforcement an opportunity to prevent harm to potential victims that would not be available if the interim standard's lack of timing requirements were left unaltered.

94. (d) Automated delivery of surveillance status information. Action by the Commission is also warranted with respect to the delivery of surveillance status information. Section 103 of CALEA provides that a telecommunications carrier "shall ensure" that its equipment is capable of intercepting communications and isolating call-identifying information. Section 103 thereby places an affirmative obligation upon the carrier to verify that its equipment is operational and that law enforcement has access to all communications and information within the scope of the authorized surveillance.

95. Any other interpretation of Section 103's "ensure" requirement would be inconsistent with Congress' clear intent to preserve capabilities available to law enforcement prior to CALEA's

passage. Law enforcement traditionally has had the ability, when it conducts interceptions, promptly to discern, through the application of a tone to the circuit, if there is any mistake, interruption, or trouble affecting an interception delivery effort. In addition, law enforcement has had the ability to ensure that all of a subject's communications are intercepted, because it acquires sufficient signaling information to know that law enforcement is monitoring the correct subscriber.

96. The TIA interim standard does not recognize any affirmative obligation on the part of carriers to assure law enforcement that the carriers' equipment is operational. Yet absent mechanisms to ensure that a carrier's equipment is functioning, law enforcement will not be able to verify the efficacy, accuracy, and integrity of its surveillance. Without such mechanisms, all intercepted evidence will be subject to challenge as incomplete or inaccurate. Because the TIA interim standard imposes no obligation on carriers to "ensure" that their equipment is capable of isolating and delivering all relevant communications and call-identifying information within the scope of a surveillance order, the standard is deficient under CALEA.

97. In principle, carriers can provide law enforcement with necessary surveillance status information by a variety of means. In practice, the most efficient and reliable means is through the automated delivery of status reporting messages. The proposed rule therefore calls for the automated delivery of three kinds of surveillance status signals: (i) a continuity tone or signal, which would ensure that law enforcement is notified immediately if the delivery channels from the carrier have failed; (ii) a surveillance status message, which would verify that the surveillance is on the correct service and is operational; and (iii) a message reporting any changes in the service features of a

subscriber that might affect law enforcement's ability to obtain all of the communications it is entitled to acquire under a court order or other lawful authorization. The automated delivery of these signals is not the only means by which of the requirements of Section 103 could be satisfied, but it is the most practical and cost-effective means and therefore should be included in the technical requirements and standards established by the Commission. The provision of these signals will preserve law enforcement's ability, when a switch- or network-based interception is controlled by the carrier, to verify and document that all of a subject's calls and call-identifying information are being intercepted and "expeditiously" delivered.

98. (i) Continuity tone. Law enforcement can verify and document that all of a subject's calls were intercepted only if it has a means to discern promptly an interruption in an interception. The proposed rule provides for carriers to deliver "a continuity check in the form of an in-band signal * * * or tone * * * that will verify that CCCs [call content channels] between the carrier and a law enforcement agency are in working order." Appendix 1 (§ 64.1708(h)). As noted, law enforcement has the ability to deliver such a tone itself today when it conducts interceptions. If such a capability is not preserved, law enforcement will lose the ability automatically to verify the efficacy, accuracy, and integrity of an interception effort.

99. (ii) Surveillance status message. Today, law enforcement employs non-automated means to determine whether the interception device is accessing the correct equipment, service, or facility. However, digital switching will preclude law enforcement from performing this function because law enforcement will no longer have access to the intercept location. The proposed rule therefore

provides for the automated delivery of surveillance status messages. Appendix 1 (§ 64.1708(f)). The rule provides for surveillance messages to be triggered and delivered "whenever a surveillance is activated, updated, or deactivated," and "periodically from once every hour to once every 24 hours for the duration of a surveillance." Id. § 64.1708(f)(1)-(2). The receipt of surveillance status messages would indicate that the interception is working correctly and is accessing the correct subscriber's service. It would also confirm that the path over which the message was sent is still operational. Without this information, law enforcement would not know when the software is turned on or off, or if it has failed. Law enforcement could not verify that the subject is being monitored, leaving open the possibility that important evidence is being lost. Providing this message will enable law enforcement to quickly correct any faults in the implementation of an interception.

100. Absent an automated surveillance status message, an interception could be overridden inadvertently or removed by carrier personnel for hours or days without law enforcement's knowledge. This circumstance could occur even with a continuity check because the continuity tone applies to the status of a call content channel or circuit, while the surveillance status message applies to the operation of the surveillance software in the switch. Thus, without surveillance status messages, law enforcement could receive an active circuit without being able to confirm that the surveillance software itself was activated and functioning properly. Further, if the subjects of surveillance cease their service or change their telephone numbers, law enforcement would be unable to obtain continuous surveillance coverage or could be put in the position of monitoring the telecommunications of an uninvolved third party.

101. (iii) Feature status message. The proposed rule also provides for automated delivery of messages indicating changes in a subscriber's call features and services (e.g., conference calling and call forwarding). Appendix 1 (§ 64.1708(g)). The provision of an appropriate automated message would enable law enforcement to procure the number of delivery channels or circuits required to ensure that the interception is fully effected and delivered as authorized. Whenever a subscriber has call forwarding or other features permitting the subscriber or another person to make multi-party calls, law enforcement must have access to multiple call content channels to ensure that it will receive all communications and call-identifying information that are subject to a court order or other lawful authorization. Without knowing what features are activated on a subscriber's service, law enforcement cannot know how many interception delivery channels and circuits are necessary. And without adequate delivery circuits, call content and call-identifying information evidence will be lost.

102. A carrier that fails to provide information on changes in a subscriber's calling features or services, in a timely manner, fails to satisfy its obligation under Section 103 to "ensure" that its equipment is capable of delivering all communications and associated call-identifying information to law enforcement. Law enforcement historically has been able to obtain this kind of information, but it has had to do so through relatively slow manual means. Because there were relatively few services or features a subscriber could choose that would affect the number of delivery channels needed for an interception effort, the fact that law enforcement received information on service changes by manual means did not significantly impair law enforcement's surveillance capabilities. In today's digital environment, however, the need for prompt notification is acute, because digital

switching has enabled customers to make rapid and instantaneous changes in their services and features, and because so many services and features trigger the need for multiple delivery channels.

103. As a practical matter, the automated nature of the foregoing features is extremely important. It would be impractical both for law enforcement and for telecommunications carriers themselves if carriers were to attempt to meet their obligations under Section 103 through a system that relied upon extensive human intervention. Under such an approach, law enforcement officials would have to contact carrier employees on a daily or hourly basis to verify these aspects for every electronic surveillance effort underway. By contrast, automating these functions would provide the information promptly and without human intervention, thereby lessening the burden on law enforcement and carriers and reducing the likelihood that critical communications and call-identifying information will be lost. Therefore, while the automated delivery of surveillance status messages is not the only possible means by which carriers can meet their obligations under Section 103, the automated surveillance status message provisions of the proposed rule represent the most appropriate way to "meet the assistance capability requirements of section 103 by cost-effective methods" (47 U.S.C. § 1006(b)(1)).

104. (e) Standardization of delivery interface protocols. In order for call content and call-identifying information to be delivered from a carrier to law enforcement, the parties must use equipment with a common delivery interface protocol. Section 103 does not obligate carriers to use any particular interface protocol, and the Department of Justice and the FBI are not asking the Commission to impose such an obligation by rule. However, a limitation on the number of interface

protocols is necessary to "ensure" that, as a practical matter, all content and call-identifying information to which law enforcement is entitled can actually be delivered. Unless a relatively small number of standardized protocols are employed, each carrier will be free to employ a separate interface protocol, and law enforcement agencies could be faced with prohibitive practical and financial burdens in equipping themselves to deal with scores of different protocols. As a practical matter, law enforcement agencies thus would be denied access to information to which they are guaranteed access by CALEA.

105. Although the interim standard contains non-binding information regarding the delivery interface protocols preferred by law enforcement, it does not contain any limitation on the number of protocols that may be used by carriers to deliver call content and call-identifying information. The proposed rule limits the number of interface protocols to no more than five. Appendix 1 (§ 64.1708(j)). Within this limit, the proposed rule leaves industry free to determine for itself which interface protocols will be used. While we are proposing a limit of five protocols, we do not mean to suggest that five is the only reasonable limit. The adoption of some reasonable limit, however, is necessary to ensure that the capability assistance requirements of Section 103 are not rendered illusory in practice by a proliferation of protocols.

3. The Technical Requirements and Standards of the Proposed Rule Satisfy the Criteria of Section 107(b) of CALEA

106. As noted above, Section 107(b) of CALEA identifies a number of criteria to be considered by the Commission in establishing technical requirements and standards. The provisions of the proposed rule meet each of these statutory criteria.

107. (a) Section 107(b)(1). The first criterion of Section 107(b) is that the technical requirements and standards "meet the assistance capability requirements of section 103" and do so by "cost-effective methods." 47 U.S.C. § 1006(b)(1). The foregoing discussion demonstrates that the provisions of the proposed rule meet Section 103's assistance capability requirements. In some instances, the requirements of the proposed rule embody the only means by which Section 103's requirements can be fully met. In other instances, while more than one mechanism or requirement might suffice to discharge a carrier's assistance obligations, the interim standard fails to mandate any such mechanism or requirement at all, and the proposed rule identifies a reasonable means of ensuring that those capability requirements are met.

108. The Department of Justice and the FBI further believe that the provisions of the proposed rule represent cost-effective means of meeting the assistance capability requirements of Section 103. A precise assessment of the cost-effectiveness of the proposed rule depends in part on cost information that industry, rather than law enforcement, possesses. However, during the course of discussions between law enforcement and industry over the development of standards to implement of Section 103, industry has not identified less expensive means of obtaining the results that law

enforcement believes to be required by CALEA. If it emerges during the course of this rulemaking proceeding that there are less costly alternatives that are equally effective in terms of carrying out the assistance capability requirements of Section 103, the Department of Justice and the FBI would not object to the incorporation of such alternatives in the technical requirements and standards established by the Commission.

109. In some respects, such as the selection of a limited number of standardized delivery interface protocols (part III.A.2.e supra), adoption of the proposed rule should affirmatively reduce the overall cost of implementing CALEA to industry as well as law enforcement. Moreover, many of the capabilities requested by law enforcement in this petition would merely build upon features commonly used by telecommunications carriers today in the provision of services to customers, and could therefore be implemented at incremental cost to the carriers. For example, a carrier that supports a conference calling capability uses software to keep track of who is part of a conference call and to maintain the call through conferencing bridging equipment. If a carrier already has the ability to monitor when parties are added to, placed on hold during, or dropped from the conference call, a requirement that the carrier deliver that information to law enforcement will not impose a significant cost burden. Similarly, to route calls and for billing purposes, carriers receive and interpret subject-initiated dialing activity that directs a call through the carrier's network or allows the subject to control call services. In this regard, law enforcement simply seeks access to information that the carrier necessarily processes and maintains. In addition, in seeking notification messages reflecting network-generated signaling information, law enforcement is simply asking

carriers to transmit to law enforcement information that carriers' software is already fully capable of delivering to the carriers themselves or transmitting to their subscribers.

110. (b) Section 107(b)(2). The second criterion in Section 107(b) is that the technical requirements and standards "protect the privacy and security of communications not authorized to be intercepted." 47 U.S.C. § 1006(b)(2). The capabilities and features in the proposed rule in no way jeopardize these privacy and security interests. As explained above, Title III contains numerous provisions designed to ensure that lawful surveillance does not unnecessarily intrude on the privacy of communications that are outside the legitimate scope of the criminal investigation, and CALEA itself contains additional privacy safeguards. See, e.g., 18 U.S.C. § 3121(c) (as amended by Section 207(b) of CALEA); 47 U.S.C. § 1002(a)(4)(A). In important respects, the provisions of the proposed rule actually enhance these privacy protections. For example, information on participants in a multi-party call that is conveyed by party hold and party join messages enhances privacy because law enforcement can more readily avoid recording conversations that are not of a criminal nature. Similarly, receipt of surveillance status messages ensures that the interception software is working correctly and is not accessing the service of an innocent subscriber. And the delivery of all call-identifying information, including post-cut-through dialed digits, over a call data channel would obviate the need to access a call content channel when law enforcement agencies are seeking only call-identifying information.

111. (c) Section 107(b)(3). The third criterion in Section 107(b) is that the technical requirements and standards "minimize the cost of * * * compliance on residential ratepayers." 47 U.S.C.

§ 1006(b)(3). The Department of Justice and the FBI believe that the provisions of the proposed rule impose the least financial burden on residential ratepayers consistent with the underlying need to meet the assistance capability requirements of Section 103, and industry has not indicated otherwise in prior discussions regarding the implementation of Section 103. A precise assessment of the impact of the proposed rule on residential ratepayers depends in part on cost information that is in the possession of industry rather than law enforcement. If it is shown during this rulemaking proceeding that there are alternatives to the provisions of the proposed rule that are equally effective in terms of carrying out Section 103 but would result in a smaller burden on residential ratepayers, the Department of Justice and the FBI would not object to the incorporation of such alternatives in the technical requirements and standards established by the Commission.

112. It should be noted that Section 229(e)(3) of the Communications Act of 1934 (47 U.S.C. § 229(e)(3)), as amended by CALEA, requires the Commission to convene a Federal-State Joint Board to recommend the appropriate changes to Part 36 of the Commission's rules regarding the recovery of CALEA-related costs. The Commission has initiated a rulemaking in this matter,²² and in the course of the rulemaking, the Commission has addressed cost recovery issues for non-reimbursable CALEA expenditures and whether changes are required to Part 36 of the Commission's rules in this regard. The Commission has not yet ruled on this issue. Once the Federal-State Joint Board issues its recommendation and the Commission issues a decision in this matter, industry and

²² In the Matter of Jurisdictional Separations Reform and Referral to the Federal-State Joint Board, CC Docket No. 80-286 (released October 7, 1997).

law enforcement will know more about how non-reimbursed CALEA costs are to be recovered from residential ratepayers.

113. (d) Section 107(b)(4). The fourth criterion in Section 107(b) is that the technical requirements and standards "serve the policy of the United States to encourage the provision of new technologies and services to the public." 47 U.S.C. § 1006(b)(4). The provisions of the proposed rule are fully consistent with this criterion. The proposed rule does not impose any material restrictions on the adoption and provision of new technologies and services to the public by the telecommunications industry. It simply ensures that industry will take the steps necessary to carry out its statutory assistance obligations in conjunction with such technological advances.

114. (e) Section 107(b)(5). Finally, Section 107(b)(5) provides for the Commission to "provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under section 103 during any transition period." The Department of Justice and the FBI suggest that the Commission provide a reasonable time for compliance with the technical standards adopted in this rulemaking proceeding by making the standards effective 18 months after the date of the Commission's decision and order in this proceeding. The Commission should further direct that industry will designate standardized delivery interface protocols within 90 days after the date of the Commission's decision and order.

**B. THE COMMISSION SHOULD CONSIDER THIS MATTER
ON AN EXPEDITED BASIS**

115. The Commission has the authority to act on this petition on an expedited basis. Expedited consideration of a petition is warranted when a petitioning party makes a showing that it is necessary to serve the public interest. Omnipoint Corporation v. PECO Energy Company, PA 97-002, 1997 FCC LEXIS 2056, at *2 and cases cited at n.14 (Released April 18, 1997). In this case, important considerations of public safety and effective law enforcement call for expedition.

116. Expedition is warranted because effective electronic surveillance in a carrier-controlled, switch-based or network-based environment cannot be conducted without the electronic surveillance requirements set forth in this petition. This is because electronic surveillance in switch- and network-based environments depends, in great measure, upon carriers providing law enforcement the functions and capabilities that, in the past, law enforcement officers themselves could obtain. If telecommunications carriers follow only the TIA interim standard, not only will electronic surveillance information critical to criminal investigations and prosecutions be lost, but the safety of undercover officers, intercept subjects, and the public may be endangered. Thus, the deficiencies in the TIA interim standard must be remedied as soon as possible.

117. In addition, the product manufacturing and deployment schedules to produce the software and hardware necessary to comply with CALEA must be set in motion well in advance of the date that the technology actually becomes publicly available for use. If the deficiencies in the TIA interim standard are not addressed immediately, law enforcement, telecommunications carriers, and

equipment manufacturers will be uncertain as to how to proceed. Moreover, a delay in a standard that fully meets CALEA's requirements may also result in an increase in costs both to the government and to industry.

118. The CALEA-related deadlines that could be threatened by the failure to resolve the standards issue in a timely manner are set forth in the FBI's CALEA Implementation Report of January 26, 1998, which was submitted to the Chairman of the Subcommittee on Commerce, Justice, State, the Judiciary and Related Agencies, House Appropriations Committee. Appendix B to that report sets forth platform roll-out dates for five switch manufacturers, all of which include software solution availability dates in the 1998-2000 time frame.²³

²³ See CALEA Implementation Report, "Solution Availability Timeline," attached hereto as Appendix 6.

IV. CONCLUSION AND RELIEF REQUESTED

119. As the foregoing discussion demonstrates, the TIA interim standard omits electronic surveillance capabilities that are contemplated by the provisions and policies of CALEA, and the electronic surveillance information obtained through each capability is authorized under the applicable surveillance laws. Further, these capabilities are necessary for law enforcement properly and effectively to conduct electronic surveillance. In enacting CALEA, Congress intended to ensure that new technologies and services will not hinder law enforcement access to the communications content and call-identifying information that is the subject of an authorized electronic surveillance request. Absent the capabilities identified in this petition, the interim standard fails to carry out that intent and does not meet the requirements of Section 103 of CALEA.

120. For the foregoing reasons, the Department of Justice and the FBI, on behalf of themselves and other federal, state, and local law enforcement agencies, respectfully request that the Commission issue an order initiating an expedited rulemaking proceeding for the establishment of technical requirements and standards under Section 107(b) of CALEA. The Department of Justice and the FBI request that this petition be placed on public notice no later than Friday, April 27, 1998. Following the receipt of public comment on the petition, the Commission should issue a Notice of Proposed Rulemaking that proposes adoption of the provisions contained in this petition and proposed rule and/or any other requirements and standards that the Commission determines to be appropriate under Section 107(b) and the other statutory provisions applicable to this matter.

Because of the important public safety and law enforcement interests at stake, we request that the final decision and order in this matter be issued no later than September 28, 1998.

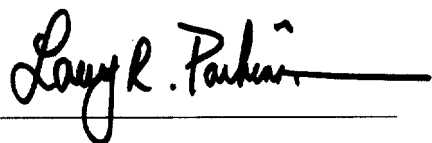
121. The Department of Justice and the FBI further respectfully request that the Commission not stay the interim standard during the consideration of the issues raised in this petition, but rather leave the interim standard in effect pending the issuance of a final decision in the rulemaking proceeding.

DATE: March 27, 1998

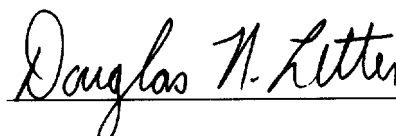
Respectfully submitted,

Louis J. Freeh, Director
Federal Bureau of Investigation

Honorable Janet Reno
Attorney General of the United States

A handwritten signature in cursive script, reading "Larry R. Parkinson", followed by a horizontal line.

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

A handwritten signature in cursive script, reading "Douglas N. Letter", followed by a horizontal line.

Stephen W. Preston
Deputy Assistant Attorney General
Douglas N. Letter
Appellate Litigation Counsel
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530
(202) 514-3602

Before the
Federal Communications Commission
Washington, D.C. 20554

Certificate of Service

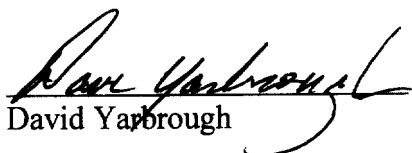
)
)
In the Matter of:)
)

Establishment of Technical Requirements
and Standards for Telecommunications)
Carrier Assistance Capabilities Under the)
Communications Assistance for Law)
Enforcement Act)
)
_____)

Docket No. _____

I, David Yarbrough, a Supervisory Special Agent in the office of the Federal Bureau of Investigation (FBI), 14800 Conference Center Drive, Suite 300, Chantilly, Virginia 20151, hereby certify that, on March 27, 1998, I caused to be served, by first-class mail, postage prepaid (or by hand where noted) copies of the above-referenced Joint Petition For Expedited Rulemaking, the original of which is filed herewith and upon the parties identified on the attached service list.

DATED at Chantilly, Virginia this 27th day of March, 1998.


David Yarbrough

**In the Matter of
Establishment of Technical Requirements and Standards
for Telecommunications Carrier Assistance Capabilities Under the
Communications Assistance for Law Enforcement Act**

Service List

***The Honorable William E. Kennard, Chairman**
Federal Communications Commission
1919 M Street, N.W.-Room 814
Washington, D.C. 20554

***The Honorable Harold Furchtgott-Roth, Commissioner**
Federal Communications Commission
1919 M Street, N.W.-Room 802
Washington, D.C. 20554

***The Honorable Susan Ness, Commissioner**
Federal Communications Commission
1919 M Street, N.W.-Room 832
Washington, D.C. 20554

***The Honorable Michael Powell, Commissioner**
Federal Communications Commission
1919 M Street, N.W.-Room 844
Washington, D.C. 20554

***The Honorable Gloria Tristani, Commissioner**
Federal Communications Commission
1919 M Street, N.W.-Room 826
Washington, D.C. 20554

***Christopher J. Wright**
General Counsel
Federal Communications Commission
1919 M Street, N.W.-Room 614
Washington, D.C. 20554

***Daniel Phythyon, Chief**
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W.-Room 5002
Washington, D.C. 20554

***David Wye**
Technical Advisor
Federal Communications Commission
2025 M Street, N.W.-Room 5002
Washington, D.C. 20554

***A. Richard Metzger, Chief**
Common Carrier Bureau
Federal Communications Commission
1919 M Street, N.W.-Room 500B
Washington, D.C. 20554

***Geraldine Matise**
Chief, Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 235
Washington, D.C. 20554

***Kent Nilsson**
Deputy Division Chief
Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 235
Washington, D.C. 20554

***David Ward**
Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 210N
Washington, D.C. 20554

***Marty Schwimmer**
Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 290B
Washington, D.C. 20554

***Lawrence Petak**
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W.-Room 230
Washington, D.C. 20554

*Charles Iseman
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W.-Room 230
Washington, D.C. 20554 Policy Division

*Jim Burtle
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W.-Room 230
Washington, D.C. 20554

Matthew J. Flanigan
President
Telecommunications Industry Association
2500 Wilson Boulevard
Suite 300
Arlington, VA 22201-3834

Tom Barba
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036-1795

Thomas Wheeler
President & CEO
Cellular Telecommunications Industry Association
1250 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20036

Albert Gidari
Perkins Coie
1201 Third Avenue
40th Floor
Seattle, Washington 98101

Jay Kitchen
President
Personal Communications Industry Association
500 Montgomery Street
Suite 700
Alexandria, VA 22314-1561

Roy Neel
President & CEO
United States Telephone Association
1401 H Street, N.W.
Suite 600
Washington, D.C. 20005-2164

Alliance for Telecommunication Industry Solutions
1200 G Street, N.W.
Suite 500
Washington, D.C. 20005

*International Transcription Service, Inc.
1231 20th Street, N.W.
Washington, D.C. 20036

***HAND DELIVERED**

APPENDIX 1 - Proposed Final Rule¹

AMENDMENTS TO THE CODE OF FEDERAL REGULATIONS

PART 64 - MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

Part 64 of Title 47 of the Code of Federal Regulations (C.F.R.) is amended as follows:

1. The authority citation for Part 64 is modified to read as follows:

AUTHORITY: 47 U.S.C. §§ 151, 154, 201, 202, 205, 218-220, 229, 332, and 1006 unless otherwise noted. Interpret or apply §§ 201, 218, 225, 226, 227, 229, 332, 48 Stat. 1070, as amended, 47 U.S.C. §§ 201-204, 218, 225, 226, 227, 229, 332, 501, 503, 1002, and 1006 unless otherwise noted.

2. The Table of Contents for Subpart Q of Part 64 is amended to add Section 64.1706 to read as follows:

§ 64.1706 **Electronic Surveillance Standards**
§ 64.1707 **Interim Standard J-STD-025 Assistance Capabilities**
§ 64.1708 **Additional Assistance Capabilities**

3. New paragraphs are added, in alphabetical order, to Section 64.1702 to read as follows:

§ 64.1702 *Definitions.* * * * For purposes of Sections 1706 through 1708 of this Part, except where otherwise noted herein, terms defined in Interim Standard TIA/EIA/IS-J-STD-025 ("J-STD-025") shall have, respectively, the meanings stated in that document.

Access: Means the technical capability to interface with a communications facility, such as a communications line, switch, or other network element so that a law enforcement agency can receive and monitor call-identifying information and call content.

Assistance Capabilities: Means the electronic surveillance services and features provided by carriers to law enforcement pursuant to Section 103 of CALEA, 47 U.S.C. § 1002, and as defined by rules promulgated by the Federal Communications Commission.

Call: Means a sequence of events beginning with an initial connection or facility request and ending with the final release of all facilities used, as defined in J-STD-025. A call may have one or more legs.

¹ This draft proposed final rule follows the formatting of the Commission's proposed Final Rule in the pending rulemaking proceeding *In the Matter of the Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213 (released October 10, 1997).